Introduction to Networks

2020/10/07 Tony Lian

Special thanks to Night for the original slides

What we are going to talk about today

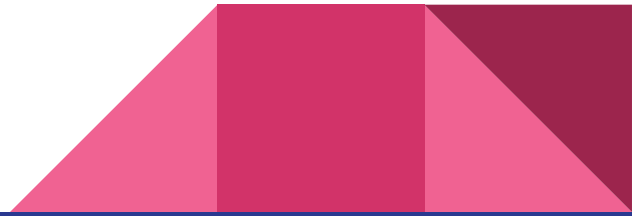
- High level overview on networking
  - MAC Address
  - IP Address & Subnetting
  - Routing
  - DNS
  - TCP
- Sysadmin commands and Technical demos (live)
  - A lot of commands
  - How to read a traceroute

Intro to networks

What are networks for? Communication!

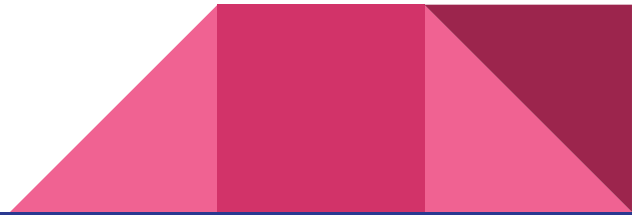
Seems easy but really complicated:

- Easily identify a computer
- Low latency
- High throughput (bandwidth)
- Low packet loss
- Fault-tolerant
- (More desirable properties…)



MAC addresses

- **Media access control (MAC)** addresses are identifiers uniquely assigned to network interfaces
- Referred to as the **physical address**
- **48 bits**, often written in hexadecimal octets (i.e. b6)
- An example MAC address is 74:d4:35:43:1e:e7
- The first 3 octets refer to the Organizationally Unique Identifier (OUI)
  - 74:d4:35 is GIGA-BYTE TECHNOLOGY CO.,LTD.
  - See http://standards-oui.ieee.org/oui.txt for a full list
- MAC addresses are only useful on the **same local network**
  - How do we get across the wider Internet?

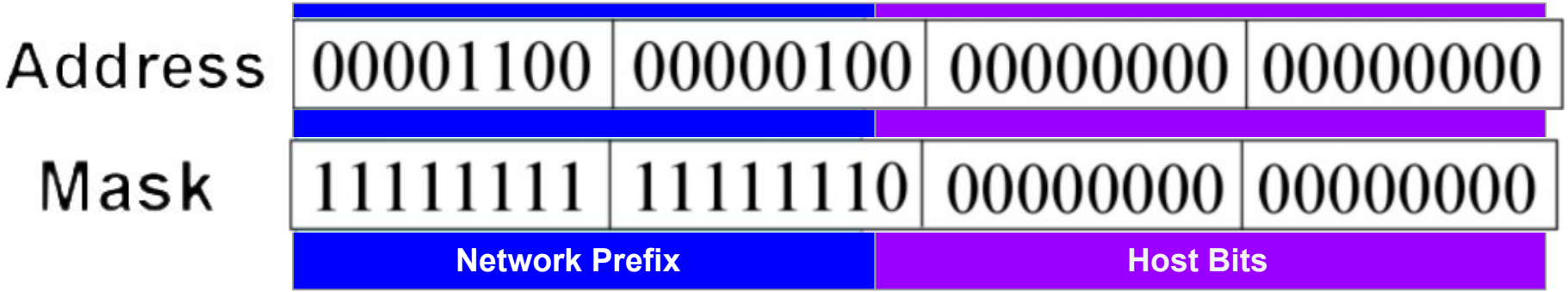


IP addresses & Subnetting

- An IP address uniquely identifies a host
- IPv4: 32 bits, formatted like 123.45.67.89
  - There are only 4.3 billion IPv4 addresses (and some are reserved)
  - There are 7.7 billion people 🤔 🤔 🤔 How do we solve it?
  - NAT: Network Address Translation
- IPv6: 128 bits (4x), formatted like 1234:5678:89:0:ab:cd:ef:beef
  - Now we have a million billion IP addresses for each cell in every human on the planet (a lot)
- Subnet: a range of IP addresses (e.g. 192.168.1.0-255)
  - CIDR: 192.168.1.0/24
  - The “mask” is the first 24 bits of 192.168.1.1. The last 8 bits can differ.
  - 11000000.10101000.00000001.xxxxxxxx
  - 11000000.10101000.00000001.01100100 = 192.168.1.100 is in the subnet

CIDR walkthrough

- Suppose we have the subnet 12.4.0.1/15.
- 12.4.0.0 is the network address (Network Address = IP Address & Mask)
- 15 is the mask.



- Network prefix identifies the network that the IP address is on
- Host bits identify the host within the network
- Is 12.5.4.1 in the network? (5 = 00000101b) Yes!
- Is 12.6.4.2 in the network? (6 = 00000110b) No.

Routing

- So we have IP addresses, how do we get from one address to another?
- We jump between networks, using routing tables
- madcow (169.229.226.107):

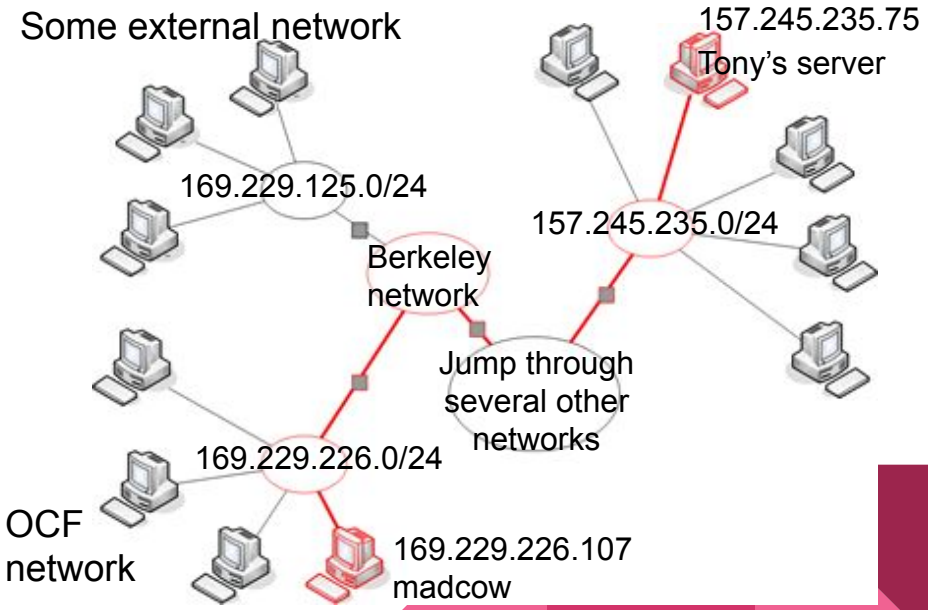
169.229.226.0/24	local network
0.0.0.0/0	via 169.229.226.1

- ocf router (169.229.226.1):

169.229.226.0/24	ocf network
169.229.0.0/16	berkeley network
128.32.0.0/16	berkeley network
0.0.0.0/0	via 128.32.0.39

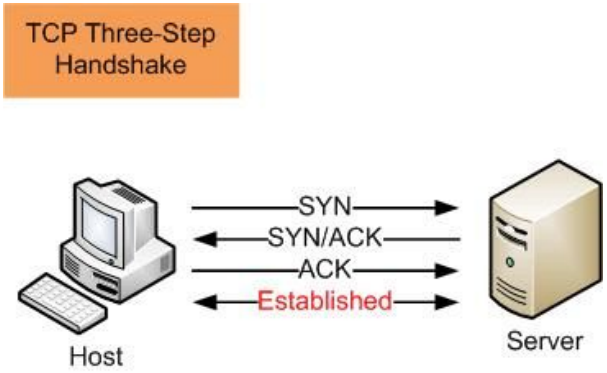
- berkeley router (128.32.0.39):

169.229.226.0/24	via 169.229.226.1



Transmission Control Protocol (TCP)

- Delivery of IP packets is not guaranteed!
- TCP is designed to resolve this problem, ensuring reliable transmission.
- Useful for websites/other non-time-critical data Transfer (HTTP/ HTTPS/ FTP use TCP)
- Sometimes time is more important than reliability
  - Any applications that apply here? Video conference.
  - TCP might not be so useful here. Instead, try UDP
    - DNS uses UDP by default
  - Ping uses ICMP, another protocol.



DNS (Domain Name System)

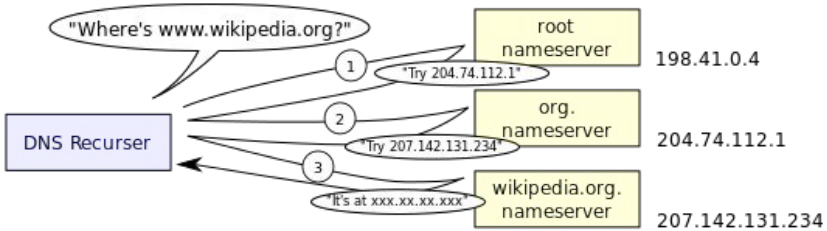
A records resolve to IPv4 addresses

AAAA records resolve to IPv6 addresses

CNAME records point to other domains

MX records designate mail servers

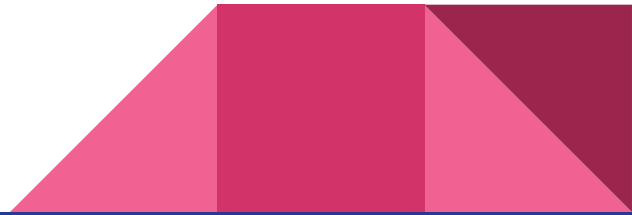
Other types of records...



Further reading: RFC 1035

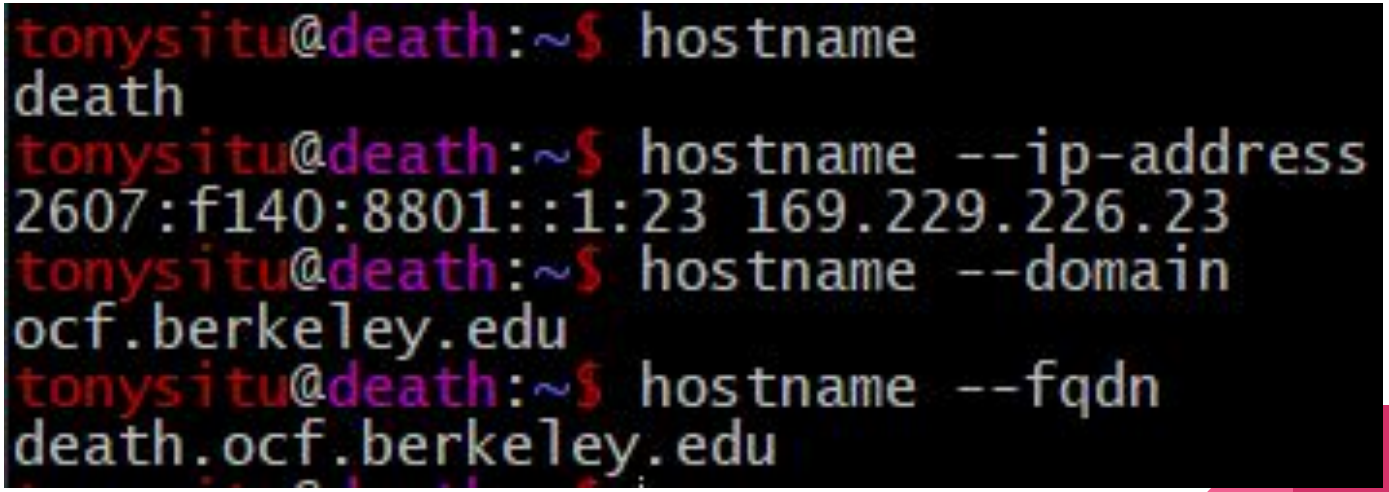
Useful tools

- hostname: get info about the current machines hostname or IP address
- host: get IP/hostname information about another machine
- ping: see if you can reach a host via an IP address
- traceroute: see the route packets take to reach a host
- arp: match local IP addresses to MAC addresses
- dig: check DNS records
- curl/wget: get files or other info over HTTP/FTP



hostname

Used to either set or display the current host, domain or node name of the system



host

Used to display hostname or IP address information about other hosts.

```
cooperc@headcrash ~ > host ssh.ocf.berkeley.edu
ssh.ocf.berkeley.edu is an alias for tsunami.ocf.berkeley.edu.
tsunami.ocf.berkeley.edu has address 169.229.226.25
tsunami.ocf.berkeley.edu has IPv6 address 2607:f140:8801::1:25
cooperc@headcrash ~ > host 169.229.226.107
107.226.229.169.in-addr.arpa domain name pointer madcow.OCF.Berkeley.EDU.
cooperc@headcrash ~ >
```

ping

Test whether a host is accessible.

Uses a protocol called ICMP.

```
staff3@staff3:~$ ping ocf.berkeley.edu
PING ocf.berkeley.edu (169.229.226.23) 56(84) bytes of data.
64 bytes from death.OCF.Berkeley.EDU (169.229.226.23): icmp_seq=1 ttl=48 time=4.00 ms
64 bytes from death.OCF.Berkeley.EDU (169.229.226.23): icmp_seq=2 ttl=48 time=4.30 ms
64 bytes from death.OCF.Berkeley.EDU (169.229.226.23): icmp_seq=3 ttl=48 time=3.40 ms
64 bytes from death.OCF.Berkeley.EDU (169.229.226.23): icmp_seq=4 ttl=48 time=3.43 ms
^C
--- ocf.berkeley.edu ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 3.401/3.783/4.300/0.389 ms
staff3@staff3:~$
```

traceroute

Print the route that a packet takes to the destination

```
tonysitu@death:~$ traceroute google.com
traceroute to google.com (216.58.194.206), 30 hops max, 60 byte packets
 1  vlan635.inr-350-reccev.berkeley.edu (169.229.226.1)  1.199 ms  0.958 ms  0.970 ms
 2  t6-6.inr-202-reccev.berkeley.edu (128.32.0.218)  0.623 ms  0.748 ms  0.675 ms
 3  xe-5-2-0.inr-001-sut.berkeley.edu (128.32.0.66)  0.573 ms  0.590 ms  0.579 ms
 4  xe-4-0-0.inr-002-reccev.berkeley.edu (128.32.0.69)  0.578 ms  0.580 ms  0.561 ms
 5  oak-agg4--ucb-10g.cenic.net (137.164.50.30)  2.418 ms  2.323 ms  2.412 ms
 6  74.125.48.172 (74.125.48.172)  3.953 ms  4.368 ms  3.000 ms
 7  108.170.242.225 (108.170.242.225)  2.930 ms  2.923 ms 108.170.243.1 (108.170.243.1)  2.912 ms
 8  108.170.237.105 (108.170.237.105)  2.987 ms 108.170.237.107 (108.170.237.107)  3.196 ms  3.175 ms
 9  sfo03s01-in-f14.1e100.net (216.58.194.206)  2.944 ms  2.996 ms  2.993 ms
```

Details of the number of routers, i.e. 'hops', in the packet path.

How many router hops away is madcow from tsunami? Hint: They are both on the same network (OCF)

arp

Match IP addresses with MAC addresses

```
tonysitu@death:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
dhcp-169-229-226-186.OC  ether   2c:0e:3d:9f:84:e3   C                     eth0
dhcp-169-229-226-185.OC  ether   00:0a:f5:8c:8a:44   C                     eth0
dhcp-169-229-226-160.OC  ether   00:21:cc:6e:08:89   C                     eth0
dhcp-169-229-226-165.OC  ether   9c:f4:8e:9d:a7:a4   C                     eth0
dhcp-169-229-226-166.OC  ether   d0:fc:cc:38:e9:91   C                     eth0
dhcp-169-229-226-171.OC  ether   48:45:20:b3:4e:4e   C                     eth0
dhcp-169-229-226-172.OC  ether   9c:b6:d0:0a:9a:9f   C                     eth0
overheat.OCF.Berkeley.E  ether   b8:27:eb:28:7a:f0   C                     eth0
firewhirl.OCF.Berkeley.  ether   1c:87:2c:72:25:1c   C                     eth0
```

dig

Utility for doing DNS queries and diagnosing DNS issues

```
staff3@staff3:~$ dig ocf.berkeley.edu

; <<>> DiG 9.11.3-1ubuntu1.8-Ubuntu <<>> ocf.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34138
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;ocf.berkeley.edu.              IN      A

;; ANSWER SECTION:
ocf.berkeley.edu.       225     IN      A       169.229.226.23

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Oct 01 02:11:50 UTC 2019
;; MSG SIZE  rcvd: 61

staff3@staff3:~$
```

wget/ curl

Transfer (upload, download, delete, etc.) things with protocol such as HTTP, HTTPS, FTP.

Really useful, and to know more: man pages.

```
longlian@supernova:~$ curl https://raw.githubusercontent.com/0xcf/decal-web/aecd69a3969f5ca495c5134e4e6bb0e0f5cc99ab/labs/b5.md
head -10
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0---
title: Lab 5 - Introduction to Networking
layout: lab
---

## Overview
It is undeniable that the internet is an important system that has redefined our world. The ability to develop networks and all
w devices to communicate is critical to modern day computer systems.  This lab will take a look into the basics of computer net
orking and then examine networks through the perspective of a sysadmin.

We will be using web browsing as an analogy to understand the basics of networking. What exactly happens when I go web browsing
for cat pictures?

 79 22944   79 18301    0     0   107k      0 --:--:-- --:--:-- --:--:--  108k
curl: (23) Failed writing body (842 != 2759)
longlian@supernova:~$
```